Claims

1. A scalable media access portal providing connectivity to network attached data storage, said scalable media access portal comprising:

a) a first network interface processor coupleable to a first network;

b) a second network interface processor coupleable to second network;

c) an array of media access processors including an assigned media access processor operative to terminate a first network media access connection relative to said first network and provides a second network media access connection relative to said second network as a proxy for said first network media access connection; and

d) a switch providing data paths between said first and second network interface processors and said array of media access processors, wherein said first network interface processor is operative to selectively route network data associated with said first network media access connection from said first network to said assigned media access processor.

2. The scalable media access portal of Claim 1 wherein said first network media access connection is a state-full connection, wherein said assigned media access processor maintains state-data reflective of the dynamic state of said first network media access connection, and wherein said assigned media access processor is responsive to said state-data in maintaining said second network media access connection.

3. The scalable media access portal of Claim 2 wherein assigned media access processor implements a transaction protocol state-machine to maintain said second network media access connection in a predetermined correspondence with said first network media access connection.

4. The scalable media access portal of Claim 3 wherein the network data selectively routed by said first network interface processor include network media data packets containing information specific to the transport of media-level data and wherein said assigned media access processor inspects network media data packets to obtain said state-data.

5. The scalable media access portal of Claim 4 further comprising a shared state-data store accessible by said array of media access processors, wherein said array of media access processors selectively update said shared state-data store, and wherein said assigned media access processor is responsive to said state-data accessed from said shared state-data store in maintaining said second network media access connection.

6. The scalable media access portal of Claim 1 wherein network data associated with said first and second network media access connection includes network data packets encapsulating media-level data and wherein said assigned media access processor provides for the encryption of media-level data within network data packets.

7. The scalable media access portal of Claim 6 wherein said assigned media access processor provides for the proxy transfer of first network data packets from

said first network media access connection to said second network media access connection as second network data packets, said assigned media access processor providing for the selective encryption of media-level data within said second network data packets based on the proxy determined destination of said second network data packets.

8. The scalable media access portal of Claim 7 wherein said assigned media access processor provides for the proxy transfer of second network data packets from said second network media access connection to said first network media access connection as said first network data packets, said assigned media access processor providing for the selective decryption of media-level data from said second predetermined network data packets.

9. The scalable media access portal of Claim 8 wherein said assigned media processor maintains coordinated the state of said first and second network media access connections to manage the proxy transfer of first and second network data packets between said first and second networks.

10. The scalable media access portal of Claim 9 wherein said first and second network data packets include media data transport state information and wherein said assigned media processor is responsive to said media data transport state information to maintain the coordination of said first and second network media access connections.

11. A secure storage access portal provided in a network between client systems and network attached data storage, said secure storage access portal comprising:

a) a data packet processor, including an encryption engine, operative to selectively encrypt a media data portion of network data packets provided to said data packet processor; and

b) a network interface processor coupleable to a client network and a storage network and coupled to said data packet processor to transfer network data packets, said network interface processor operative to associate a persistent network data route between said client and storage networks through said data packet processor such that network data packets associated with said persistent network data route are selectively passed to and from said data packet processor by said network interface processor.

12. The secure storage access portal of Claim 11 further comprising a data packet processor array that includes said data packet processor, wherein said network interface processor is operative to selectively associate a plurality of persistent network data routes with said data packet processor.

13. The secure storage access portal of Claim 12 wherein said plurality of persistent network data routes are uniquely associated with said data packet processor within said data packet processor array.

14. The secure storage access portal of Claim 11 wherein said data packet processor is responsive to a header portion of a predetermined network data

packet to select an encryption key for use in encrypting said media data portion of said predetermined network data packet.

15. The secure storage access portal of Claim 14 wherein said data packet processor is responsive to an identification of a data storage resource provided by said predetermined network data packet to select said encryption key.

16. A secure storage access portal providing for the routing of data transfer requests and responses between network clients and storage servers, said network media access controller comprising:

a) first network interface processor coupleable to a client network;

b) second network interface processor coupleable to a data storage network;

c) a plurality of data packet processors coupled to said first and second network interface processors, wherein each said data packet processor is operative to terminate respective client network connections routed to said plurality of data packet processors through said first network interface processor and to establish respective storage network connections through said second network interface processor, wherein each said data packet processor provides for the proxy transport of data transfer requests and responses between said client and storage network connections, and wherein each said data packet processor includes an encryption engine operative to selectively encrypt media-level data contained within data transfer requests and responses as transported from said client network connections to said storage network connections.

17. The secure storage access portal of Claim 16 further comprising a data switch provided to separately connect said first and second network interface processors with said plurality of data packet processors.

18. The secure storage access portal of Claim 17 further comprising a data store accessible by said plurality of data packet processors.

19. The secure storage access portal of Claim 18 wherein predetermined client network connections are associated as a connection session, wherein instances of said predetermined client network connections are terminated respectively by first and second data packet processors, wherein said first data packet processor is operative to provide session connection data to said data store and said second data packet processor is operative to retrieve session connection data from said data store.

20. The secure storage access portal of Claim 19 wherein said first and second network interface processors are responsive to network data packets received from said client and storage networks, said first and second network interface processors being operative to associate network data packets with said client and storage network connections and correspondingly route network data packets to the respective said data packet processors associated with said client and storage network connections.

21. The secure storage access portal of Claim 20 further comprising a control processor coupled through said data switch to said first and second network interface processors and said plurality of data packet processors, said data store

being coupled to and accessible by said plurality of data packet processors through said control processor.

22. A method of providing secure storage of media-level data as transported over a network within network data packets that encapsulate data storage packets, wherein data storage packets include storage commands, said method comprising the steps of:

a) establishing a network connection route for network data packets provided from a first network through a network data packet processor to a second network;

b) first processing a network data packet provided through said network connection route to determine a storage command contained within said network storage packet;

c) second processing said network data packet to determine a storage target resource from a data storage packet encapsulated by said network data packet; and

d) filtering, selectively based on a determined correspondence between said storage command and said storage target resource, the transport of said network data packet from said network connection route.

23. The method of Claim 22 further comprising the steps of:

a) locating within said data storage packet, selectively based on said storage command, media-level data; and

b) encrypting, selectively based on said storage target resource, the media-level data.

24. The method of Claim 23, prior to the step of encrypting, further comprising the step of compressing the media-level data, selectively based on said storage target resource.

25. The method of Claim 24 wherein said second processing step includes the step of redirecting said network data packet from said storage target resource to an alternate storage target resource.

26. The method of Claim 22 wherein said network data packet processor is one of a plurality of network data packet processors, wherein said step of establishing includes establishing respective network connection routes through said plurality of network data packet processors.

27. The method of Claim 26 wherein said respective network connection routes are persistently established through said plurality of network data packet processors.

28. The method of Claim 27 further comprising the step of third processing said network data packet to determine the selection of said network connection route from said respective network connection routes.

29. The method of Claim 28 further comprising the steps of:

a) locating within said data storage packet, selectively based on said storage command, media-level data; and

b) encrypting, selectively based on said storage target resource, the media-level data.

30. The method of Claim 29, prior to the step of encrypting, further comprising the step of compressing the media-level data, selectively based on said storage target resource.

31. The method of Claim 30 wherein said second processing step includes the step of redirecting said network data packet from said storage target resource to an alternate storage target resource.